

RFC 3833 : Threat Analysis of the Domain Name System (DNS)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 16 Novembre 2005

Date de publication du RFC : Août 2004

<http://www.bortzmeyer.org/3833.html>

Comme beaucoup de protocoles Internet, le DNS avait été conçu sans se préoccuper de la sécurité. Comme souvent, on s'aperçoit avec DNSsec que l'ajout de la sécurité à un protocole n'est pas si triviale que ça. Mais, avant de penser à la solution, il faut étudier le problème : c'est ce que fait ce RFC qui analyse les risques liés au DNS et les possibilités qu'offre ces failles aux fraudeurs.

Modifier des réponses DNS ou bien injecter de fausses réponses qui seraient acceptées par les clients permet en effet nombre d'attaques, comme de rediriger les requêtes censées aller au serveur d'une banque vers le serveur d'un méchant qui copierait les mots de passe.

Il faut noter que le RFC ne parle que des faiblesses du protocole, pas des bogues des mises en œuvre.

Enfin, rappelons que beaucoup d'attaques d'usurpation ne nécessitent pas de faille du DNS : ces attaques peuvent simplement exploiter la crédulité ou bien la distraction de l'utilisateur. D'où l'importance de mesures de sécurité comme celles de SSH qui contrôle la clé cryptographique du serveur où il se connecte.

Le RFC note que les attaques suivantes sont possibles :

- Interception des paquets (questions ou réponses) et émission par l'attaquant d'un autre paquet. Tous les protocoles permettent cela mais c'est plus facile avec le DNS, où question et réponse tiennent souvent dans un seul paquet chacune. Cela nécessite en général que l'attaquant soit situé entre le client et le serveur.
- Fabrication d'une réponse vraisemblable. Cela peut se faire en devinant l'ID (un numéro choisi par le client DNS et qui lui permet de mettre en correspondance requêtes et réponses) d'une requête (et le nom demandé), ce que la faible taille des ID (16 bits) rend possible.

- Chainage de noms, une technique qui consiste à injecter des données dans le cache de la victime en utilisant une indirection. Par exemple, une réponse de type NS ("*name server*") va entraîner des requêtes dans un domaine potentiellement complètement différent, pour résoudre les noms en partie droite de la réponse.
- Trahison par un serveur : si je branche mon portable sur un réseau que je ne contrôle pas, le serveur cache de ce réseau peut envoyer à ses clients des données mensongères. Même chose si un des secondaires d'un domaine décide de tricher, alors qu'il devrait n'envoyer que ce qu'a décidé son primaire.
- Déni de service

Le RFC discute également des problèmes qui ne sont pas des vulnérabilités à proprement parler mais qui compliquent la solution de sécurité, comme la nécessité de pouvoir signer la non-existence d'un domaine ou bien les jokers ("*wildcards*"), qui compliquent tant de protocoles liés au DNS.

Le RFC se termine par une discussion des problèmes liés à DNSsec lui-même (DNSsec ne résoud pas toutes les failles de sécurité du DNS).